ict unie

SPRÁVA A UKLÁDÁNÍ DŮVĚRYHODNÝCH DOKUMENTŮ

Stanovisko ICT UNIE

ICTU 2016

Obsah

Poznámka autorského kolektivu

Při tvorbě tohoto dokumentu autoři vycházeli ze současné právní úpravy a technických standardů ČR a EU, ze zkušeností a praxe různých členských států EU a také z historických zvyklostí a právních premis.

V textu je také používán pojem „archiv“. Tento termín je použit ve volnějším kontextu v souladu s obecně zažitou terminologií.

Autoři si jsou vědomi, že „důvěryhodnost“ konkrétního dokumentu jakožto důkazního prostředku v soudním řízení může určit pouze soud.

Termín	Význam
AdES	Advanced Electronic Signature (Direktiva EU 1999/93/EC) – skupina standardů definujících podobu rozšířených elektronických podpisů (CAdES, XAdES, PAdES).
Archivní balíček	Archival Information Package (nebo také AIP) je definovaný normou ISO 14721:2012 – Open Archival Information System (nebo také OAIS). Jedná se o dokument(y) a jeho metadata zabalené do XML obálky.
Autentický	Původní, pravý.
Bezpečnostní prvek	Elektronický podpis, elektronická značka, časové razítko (a jejich kvalifikované certifikáty), CRL listy, validační zpráva a OCSP protokol.
Certifikát	Certifikátem se rozumí datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování elektronických podpisů s podepisující osobou a umožňuje ověřit její identitu nebo spojuje data pro ověřování elektronických značek s označující osobou a umožňuje ověřit její identitu.
CRL	Certificate revocation list – seznam zneplatněných certifikátů vydávaný a podepsaný certifikační autoritou.
Časové razítko (kvalifikované)	Kvalifikovaným časovým razítkem se rozumí datová zpráva, kterou vydal kvalifikovaný poskytovatel certifikačních služeb a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem.
Čitelnost	Čitelností elektronického dokumentu rozumíme možnost získat datový obsah uložený v dokumentu. Dokument uložený jako elektronický nebo jiný záznam v analogové nebo digitální formě není přímo čitelný člověkem, ale vyžaduje technické a případně i softwarové prostředky pro čtení nebo vizualizaci.
Datová zpráva	Jedná se o elektronická data, která lze přenášet prostředky pro elektronickou komunikaci (např. informační systém datových schránek) a uchovávat na technických nosičích dat, používaných při zpracování a přenosu dat elektronickou formou, jakož i data uložená na technických nosičích ve formě datového souboru.
Digitální dokument	Digitálním dokumentem se rozumí dokument v elektronické podobě; viz také elektronický dokument.
Dokument	Podle § 2 písm. e) zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů, každá písemná, obrazová, zvuková nebo jiná zaznamenaná informace, ať již v podobě analogové, či digitální, která byla vytvořena původcem nebo byla původci doručena. Dokument má tedy obecnější podobu než písemnost, neboť předpokládá více forem než pouze písemnou. Podle platné právní úpravy musí být právní úkon podepsán jednající osobou vlastnoručně. V případech, kdy je to obvyklé, může být nahrazen mechanickými prostředky (např. razítkem). Je-li právní úkon učiněn elektronicky, může být podepsán zaručeným elektronickým podpisem.

TERMINOLOGIE

Termín	Význam
Doručování	Různé způsoby odesílání a poskytování dokumentů: zasílání prostřednictvím odesílajících a přijímacích subjektů, zasílání konzulární nebo diplomatickou cestou, prostřednictvím poštovních služeb a přímým doručením. Odesílající subjekty odpovídají za odesílání soudních a mimosoudních dokumentů doručovaných do jiného členského státu. Přijímající subjekty odpovídají za příjem soudních a mimosoudních dokumentů z jiného členského státu. Ústřední orgán poskytuje informace odesílajícím subjektům a hledá řešení veškerých obtíží, které mohou vzniknout při zasílání písemností určených k doručení.[1]
Důvěra	Důvěra je spolehnutí se na něco, očekávání něčeho, je určující faktor v procesu rozhodování. Znamená vztah spoléhání na druhé lidi, instituce nebo věci.
Důvěryhodnost	Důvěryhodnost je vlastnost vztažená k nabízené nebo poskytované službě, ze které je možno odvodit důvěru v řádné provedení této služby.
Elektronická značka	Elektronickou značkou se rozumí údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které splňují následující požadavky: 1. jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřednictvím kvalifikovaného systémového certifikátu, 2. byly vytvořeny a připojeny k datové zprávě pomocí prostředků pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou, 3. jsou k datové zprávě, ke které se vztahují, připojeny takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat.
Elektronický dokument	Elektronickým dokumentem se rozumí dokument v elektronické podobě.
Elektronický podpis	Elektronickým podpisem se rozumí údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě.
Fixace	Stav dokumentu, ve kterém je daný dokument již nadále obsahově neměnný.
Integrita dokumentu	Integritou rozumíme neporušenost původního dokumentu, zejména skutečnost, že nedošlo k neoprávněné změně informace obsažené v dokumentu.
Kolizní situace	Jedná se o stav, kdy daný dokument nesplňuje kritéria pro dokončení fáze karantény (např. neúplná povinná metadata). Tento stav vyžaduje zásah správce archivu, který stav napraví nebo rozhodne o dalším postupu (viz NSESSS, kap. 2.2 Matice příkladů rolí v rámci ERMS).
Kontextuální odkaz	Odkaz na dokument, který je s daným dokumentem v určitém obsahovém nebo logickém vztahu.
Kvalifikovaný certifikát	Kvalifikovaným certifikátem se rozumí certifikát, který má náležitosti podle § 12 zák. č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů, a byl vydán kvalifikovaným poskytovatelem certifikačních služeb.

1 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32007R1393:CS:NOT

Termín	Význam
Listina	České právo nedefinuje, jakým materiálem je listina tvořena. Obecně se má za to, že listinou je papír nebo jakýkoli jiný hmotný substrát, na němž lze zachytit písemný obsah. Za listiny po roce 1850 se pro účely evidence archiválií jako jednotliviny nepovažují dokumenty zakládající právní akty uvedené v primárních registrech, jmenování čestným občanem, výuční listy, osobní doklady, školní vysvědčení, diplomy, statuty a stanovy spolků. Jako listiny se rovněž neevidují a nevykazují cenné papíry. Jako listiny po roce 1850 se neevidují listiny, které jsou součástí spisů.[2]
Metadata	Data popisující kontext, obsah a strukturu dokumentů nebo jiných entit a jejich spravování v čase. Povinná metadata je nutné vyplnit vždy, protože podléhají automatické kontrole na vstupu do systému. Nepovinná metadata kontrolována nejsou.
Omezení rozsahu důvěryhodnosti	Každý dokument prochází určitým životním cyklem, od svého vzniku přes používání, autorizované změny, archivaci po skartaci. Pro účely tohoto dokumentu je rozhodující okamžik, kdy jsou zafixovány všechny 4 požadavky na důvěryhodný dokument, zpravidla při jeho uložení do systému pro správu důvěryhodných dokumentů. V zákoně č. 499/2004 Sb. je zakotvena právní domněnka pravosti dokumentů, což je z mnoha důvodů nebezpečná konstrukce.
Písemná forma právních jednání (písemnost)	§ 562 zákona č. 89/2012 Sb., občanský zákoník: Odst. 1: Písemná forma je zachována i při právním jednání učiněném elektronickými nebo jinými technickými prostředky umožňujícími zachycení jeho obsahu a určení jednající osoby. Odst 2: Má se za to, že záznamy údajů o právních jednáních v elektronickém systému jsou spolehlivé, provádějí-li se systematicky a posloupně a jsou-li chráněny proti změnám. Byl-li záznam pořízen při provozu závodu a dovolá-li se jej druhá strana k svému prospěchu, má se za to, že záznam je spolehlivý. (Pozn.: Účinnost od 1. ledna 2014.)
Původce	Původcem je každý, z jehož činnosti dokument vznikl; za dokument vzniklý z činnosti původce se považuje rovněž dokument, který byl původci doručen nebo jinak předán.
Původ dokumentu	Původem dokumentu rozumíme identifikaci entity, z jejíž činnosti dokument vznikl, a další atributy, které umožňují jednoznačně identifikovat dokument v kontextu jeho vzniku nebo přijetí.
Replika digitálního dokumentu	Replikou se pro účely péče o archiválii v digitální podobě rozumí řetězec znaků totožný s dokumentem v digitální podobě, z něhož byl vytvořen.
Relevantní výběr	Splňuje určitou míru shody mezi zadaným klíčem (vyhledávacími údaji) a nalezenou referencí (seznamem relevantních dokumentů).
SIP	Submission Information Package – informační objekt vstupující do archivu ze zdrojového systému (na počátku archivačního životního cyklu dokumentu) dle definice OAIS. Součástí SIP balíčku je jeden nebo více dokumentů a jejich metadata.
Skartační řízení	Skartačním řízením se rozumí proces vyřazování dokumentu z fondu organizace, který se řídí skartačním režimem.

2 Vyhláška č. 645/2004 Sb., kterou se provádějí některá ustanovení zákona o archivnictví a spisové službě a o změně některých zákonů v platném znění – příloha č. 1.

TERMINOLOGIE

Termín	Význam
Skartační návrh	Skartačním návrhem se rozumí návrh organizace na výběr a vyřazení archiválií a skartaci dokumentů s uplynulou skartační lhůtou, které nejsou nadále provozně nebo správně potřebné. Součástí skartačního návrhu je seznam dokumentů typu „A“ (tzv. archiválie) a seznam dokumentů s uplynulou skartační lhůtou se skartačními znaky S a V. Skartační návrh může být předkládán k posouzení a schválení věcně a místně příslušnému státnímu archivu pověřenému dohledem na výběr archiválií a vyřazování dokumentů organizace navrhovaných ke skartaci.
Skartační režim	NSESSS[3]: Skartační režim je organizací stanovený systém vyřazování entit, který vymezuje dobu jejich ukládání (skartační lhůta) a určuje typ skartační operace (trvalé uložení, předložení k přezkumu, automatické zničení, zničení po jeho schválení uděleném správcem nebo export do archivu). Při posouzení se v rámci odborné prohlídky vyhodnocují a) metadata, b) obsah dokumentu nebo c) metadata a obsah dokumentu. V případě, že skartační režim uplatňuje určený původce zřizující správní archiv podle § 69 odst. 1 zákona č. 499/2004 Sb., nepovažuje se podle § 69 odst. 4 zákona předání dokumentů ze spisovny do správního archivu za skartační operaci a lhůta stanovená pro uložení dokumentů ve spisovně ve spisových řádech není skartační lhůtou; pro převod dokumentu mezi spisovnami (například po odtajnění spisu) platí část věty před středníkem obdobně.
Skartační znak	§ 2 písm. r) zákona č. 499/2004 Sb.: Označení dokumentu, podle něhož se dokument posuzuje ve skartačním řízení.
Spin-down	Vlastnost diskového úložiště, umožňující vypínat elektroniku jednotlivých pevných disků na základě definovaných parametrů – např. doba nečinnosti (doba, kdy disk nebyl používán pro zápis nebo čtení dat).
Spisový a skartační plán	§ 66 odst. 2 zákona č. 499/2004 Sb.: Spisový a skartační plán obsahuje seznam typů dokumentů roztříděných do věcných skupin s vyznačenými spisovými znaky, skartačními znaky a skartačními lhůtami.
Spolehlivost	Věrohodnost, solidnost.
Stejnopis	§ 16 odst. 3 vyhlášky č. 259/2012 Sb., o podrobnostech výkonu spisové služby: Stejnopisem je jedno ze shodných násobných vyhotovení dokumentu nesoucí s tímto dokumentem shodné autentizační prvky; za shodné násobné vyhotovení dokumentu v analogové podobě se považuje rovněž doslovně shodné vyhotovení dokumentu v digitální podobě a naopak, pokud autentizační prostředky k nim připojila tatáž osoba; za stejnopis se považuje rovněž druhopis, pokud tak stanoví jiný právní předpis.
Určený původce	Původce, který má dle zákona povinnost vést spisovou službu tak, jak stanoví § 63 zákona č. 499/2004 Sb., v platném znění.

3 VMV částka 64/2012 (část II), národní standard pro elektronické systémy spisové služby.

Termín	Význam
Uznávaná elektronická značka	Uznávanou elektronickou značkou se rozumí elektronická značka založená na kvalifikovaném systémovém certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb.
Uznávaný elektronický podpis	Uznávaným elektronickým podpisem se rozumí: a) zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb a obsahujícím údaje, které umožňují jednoznačnou identifikaci podepisující osoby, b) zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném poskytovatelem certifikačních služeb, který je usazen mimo území České republiky, byl-li kvalifikovaný certifikát vydán v rámci služby vedené v seznamu důvěryhodných certifikačních služeb jako služba, pro jejíž poskytování je poskytovatel certifikačních služeb akreditován, nebo jako služba, nad jejímž poskytováním je vykonáván dohled podle předpisu Evropské unie.
Validace	Ověření integrity dokumentu, kompletnosti metadat a stavu bezpečnostních prvků.
Věrohodnost	Hodnověrnost, spolehlivost.
XAdES	XML Advanced Electronic Signatures je rozšířením standardu XML-DSig, který slouží k podepisování XML dokumentů. Definován ETSI TS 101 903.
XML	Extensible Markup Language – obecný značkovací jazyk.
Vyřazování dokumentů	Jedná se o proces, v jehož průběhu se posuzují dokumenty určené k vyřazení a na jehož konci je dokument předán do nadřízeného archivu, skartován nebo mu je posunuta skartační lhůta.
Zaručený elektronický podpis	Zaručeným elektronickým podpisem se rozumí elektronický podpis, který splňuje následující požadavky: 1. je jednoznačně spojen s podepisující osobou, 2. umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě, 3. byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou, 4. je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat.

1. MANAŽERSKÝ SOUHRN

Míra používání dokumentů v digitální podobě v České republice jednoznačně souvisí s chybějící koncepcí „důvěryhodného digitálního dokumentu“ a jasných pravidel, jak s tímto dokumentem zacházet, aniž by ztratil svoji důvěryhodnost. Tato koncepce se musí týkat nejen státní správy a samosprávy, ale hlavně komerční sféry a fyzických osob. Pouze v případě, že si digitální dokument získá všeobecnou důvěru a bude akceptován širokou veřejností, lze hovořit o zásadní elektronizaci státní správy, obchodu a průmyslu. Pracovní skupina Archivnictví ICT UNIE se proto rozhodla na tuto potřebu reagovat a zpracovat soubor dokumentů, který by důvěryhodný dokument definoval, popsal možnost jeho správy a obsahoval návrh standardu sloužícího k prokazování důvěryhodnosti dokumentu.

Prvním výsledkem byl dokument s názvem „Důvěryhodný digitální dokument – Stanovisko ICT UNIE k problematice právně validního dokumentu“ z roku 2014, který je k dispozici na webových stránkách ICTU.

Navazující částí je pak „Správa a ukládání důvěryhodných dokumentů“, kterou právě držíte v ruce. Vnímáme, že rozhodující vliv na legislativu a tím i na digitální dokumenty má a bude mít zejména „eIDAS“, který však je ve své podstatě poměrně obecným dokumentem. Proto je účelem této publikace přiblížit čtenářům to podstatné, tzn. základy, o které se bude možné prakticky opřít při běžné práci a ukládání elektronických dokumentů.

2. ÚVOD

Dlouhodobé ukládání digitálních dokumentů je oblast, kterou v současné době řeší většina moderních organizací a institucí. Je třeba zajistit, aby byly k dispozici potřebné informace vzniklé v digitální podobě a byly uchovány pro potřeby současné, ale i budoucí. Ukládání a archivace digitálních dat a dokumentů se dostává do středu pozornosti s elektronizací státní správy a firemních procesů, se zaváděním bezpapírových kanceláří a z toho plynoucím nárůstem počtu dokumentů a dat vytvořených a sdílených již pouze v digitální podobě.

Procesy a činnosti dlouhodobého ukládání dokumentů musí zajistit zaručené uložení digitálního dokumentu po prakticky neomezenou dobu – cílem je důvěryhodně uchovat digitální dokumenty především vysoké informační hodnoty, ale ne výlučně tyto. Pro řadu organizací a institucí je povinnost dlouhodobého důvěryhodného uchovávání dokumentů stanovena legislativou. Potřeba dlouhodobě důvěryhodně ukládat a uchovávat dokumenty je však zásadní i pro řadu procesů a činností v soukromoprávním sektoru.

3 SPRÁVA A UKLÁDÁNÍ DŮVĚRYHODNÝCH DOKUMENTŮ

3.1 Legislativa, normy a standardy

Oblasti správy a ukládání důvěryhodných dokumentů se dotýká řada zákonů a norem. Je třeba si uvědomit, že zatím v žádné normě ani zákonu nejsou jednoznačně, souhrnně a srozumitelně definována „pravidla“ pro „důvěryhodné“ dokumenty – jak s nimi nakládat, jak je ošetřovat i co to vlastně důvěryhodné dokumenty jsou.

V předchozí publikaci ICT UNIE – Důvěryhodný digitální dokument – Stanovisko ICT UNIE k problematice právně validního dokumentu – byla navržena definice důvěryhodného digitálního dokumentu a definovány požadavky na něj kladené. Rovněž byla shrnuta jak česká, tak evropská legislativa, které se dané problematiky dotýkají.

Pro přesnější pochopení problematiky musíme definovat podmínky – kontext, v jakém se důvěryhodné dokumenty nacházejí.

Důvěryhodný dokument můžeme chápat jako samostatnou entitu, nezávislou na prostředí, ve kterém se nachází, nebo i jako dokument, který je uložen v nějakém úložišti.

Rovněž musíme zohlednit, jakou má dokument hodnotu z hlediska historického, to znamená, jak dlouho jej budeme uchovávat.

Často se setkáváme také s pojmy „úložiště“, „garantované úložiště“, „negarantované úložiště“, „dlouhodobé úložiště“, „dlouhodobé digitální úložiště“, „dlouhodobé důvěryhodné digitální úložiště, „3D úložiště“ i „důvěryhodné úložiště“. Jaký je rozdíl v těchto pojmech? Jsou někde podchyceny jasné definice?

3.2 Souhrn legislativy – ČR

Legislativa, která se nějakým způsobem dotýká popisované oblasti, byla shrnuta v dokumentu ICT UNIE – Důvěryhodný digitální dokument – Stanovisko ICT UNIE k problematice právně validního dokumentu [2].

3.3 Souhrn legislativy – svět a EU

3.3.1 Svět

Základní úprava právních otázek spojených s elektronickou transformací a archivací byla upravena již v roce 1996 v UNCITRAL Model Law on Electronic Commerce (http://www.uncitral.org/uncitral/uncitral_texts/electronic_commerce/1996Model.html). UNCITRAL Model Law vychází ve své úpravě z důsledného technologicky neutrálního přístupu a z rozlišení pojmu „písemnost“, „originál“, „podpis“,„úřední/notářské ověření“, „právní účinek / důkazní síla“ a „archivace dokumentů“. V podstatě lze uvést, že UNCITRAL Model Law definuje „písemnost“ na nejnižší úrovni požadavků jako cokoliv v jakékoliv formě a na jakémkoliv nosiči, co je možno reprodukovat a číst pro účely budoucího využití.

Za písemnost by tedy měly být považovány např. veškeré e-mailové zprávy nebo libovolné texty v elektronické formě, bez ohledu na úroveň jejich zabezpečení nebo na to, zda je z nich patrný jejich zdroj.

Dále UNCITRAL Model Law definuje pojem „originál“, a to nikoliv ve vztahu k formě, v jaké byl příslušný dokument původně pořízen, ale ve vztahu k integritě obsahu příslušného dokumentu. Za originál by tedy bylo možno považovat i n-tou elektronickou kopii dokumentu, pokud by bylo možné prokázat integritu jejího obsahu od okamžiku, kdy byla vyhotovena ve své finální formě.

Ve Francii a Velké Británii je toto ustanovení UNCITRAL Model Law komentováno v tom smyslu, že je obtížné mluvit v moderní době o originálu dokumentu v elektronické formě a že je lépe pojem originálu vůbec opustit. Naopak, je třeba se zaměřit na stanovení obecných podmínek, za nichž mají dokumenty v libovolné formě (papírové či elektronické či jiné) plný právní účinek / důkazní sílu, srovnatelnou i s originály papírových dokumentů. Při splnění takovýchto podmínek by potom bylo možné předložit např. soudu elektronický dokument obsahující informace z původně papírového dokumentu a soud by tomuto elektronickému dokumentu měl přisoudit shodný právní účinek jako originálnímu papírovému dokumentu. Problém při tomto pojetí vzniká tam, kde právo výslovně požaduje předložení výlučně originálu. Takových ustanovení je však velmi málo a dají se upravit.

UNCITRAL Model Law uvádí obecné podmínky ovlivňující plný právní účinek / důkazní sílu elektronických dokumentů. Toto ustanovení klade důraz na zajištění integrity informací, autentičnost původce a na důvěryhodnost procesu vytváření, ukládání a komunikace datových zpráv. Splnění těchto podmínek je do značné míry ovlivněno požadavky na důvěryhodný (zaručený) elektronický podpis. UNCITRAL Model Law obsahuje požadavky na elektronický podpis v čl. 7. Vzhledem k tomu, že UNCITRAL Model Law je založen na technologické neutralitě, nebylo možné přijmout ve vztahu k elektronickým podpisům takové právní domněnky, jaké existují ve směrnici EU č. 1999/93/EC a v českém zákoně o elektronickém podpisu č. 227/2000 Sb. ve vztahu k elektronickým podpisům založeným na systému dvou klíčů. Tyto právní domněnky se právě týkají ekvivalentu s vlastnoručním podpisem (prokázání autentičnosti) a integrity obsahu. Absence právních domněnek je nyní pociťována částí odborné praxe jako nevýhoda – např. v USA, které rovněž přejaly princip technologické neutrality. UNCITRAL Model Law od těchto obecných podmínek a požadavků odlišuje elektronické úřední ověření / notarizaci. Zde pouze doporučuje, aby byly v národních zákonech odstraněny veškeré překážky znemožňující provádění úředního ověření elektronickou cestou (např. úprava požadavku aplikace úředního razítka aj.).

A konečně, UNCITRAL Model Law upravuje rovněž výslovně elektronickou transformaci a archivaci dokumentů (viz čl. 10). Úprava vychází z pojetí originálu, písemnosti a plné právní účinnosti / důkazní síly a v podstatě spojuje všechny požadavky zmiňované výše. V odst. (1) tohoto ustanovení se uvádí následující tři požadavky (skupiny požadavků) na datovou zprávu, která by měla splňovat požadavky na dlouhodobou archivaci dokumentů v libovolné formě:

– požadavky na písemnost (reprodukovatelnost a čitelnost);

– datová zpráva by měla být archivována ve formátu, v němž byla vytvořena, odeslána nebo přijata (tedy originální formát), nebo ve formátu, který umožňuje přesné zachování vytvořené, odeslané nebo přijaté informace (toto ustanovení směřuje k transformaci papírových dokumentů do elektronické formy), a

– taková informace by měla umožňovat určení původu a místa určení příslušného dokumentu a času, kdy byl dokument odeslán nebo přijat.

Použité zdroje [1],[4]

3.3.2 EU

V současné době existují a jsou platné pouze normativy, které mají formu doporučení. Jako zásadní pro definici „důvěryhodného dokumentu“ lze považovat směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy. Díky tomu, že členské státy EU tuto směrnici implementovaly odlišným způsobem, nebylo možné do současné doby sjednotit v rámci EU jak způsob tvorby a práce s důvěryhodným dokumentem, tak také jeho uznávání.

Na základě zkušeností se zaváděním výše uvedené směrnice byl zpracován nový normativ č. COM(2012) 238, návrh nařízení Evropského parlamentu a Rady o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu (eIDAS), který byl schválen dne 14. dubna 2014.

28. srpna 2014 byl tento normativ zveřejněn v úředním věstníku Evropské unie L257, svazek 57.

Nazývá se „Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES“ [3].

Je nadřazen národním legislativám a měl by tak sjednotit podmínky v rámci e-procurementu celé EU. Tento dokument bude významným krokem k uznávání důvěryhodných dokumentů. V současnosti probíhá analýza dopadů tohoto nařízení na českou legislativu.

Jedním z cílů tohoto nařízení je zajistit bezpečnou přeshraniční elektronickou identifikaci a autentizaci alespoň pro účely veřejných služeb a následně i pro podporu hospodářského a sociálního rozvoje. To by významně přispělo k řešení klíčového problému „kdo je kdo“. Zásada vzájemného uznávání by se však měla týkat pouze autentizace pro účely on-line služby.

Pilotní projekt STORK a norma ISO 29115 by měly pomoci při stanovování minimálních technických požadavků, norem a postupů pro nízkou, značnou a vysokou úroveň záruky ve smyslu tohoto nařízení.

Kromě výše uvedených dokumentů byly v rámci orgánů EU zpracovány také další normativy. Zabývají se specifickými typy dokumentů (např. elektronickými fakturami), ale také formáty a strukturou ostatních typů elektronických dokumentů.

Seznam platných normativů vydaných orgány EU v oblasti „důvěryhodného dokumentu“ je uveden v dokumentu ICT UNIE „Důvěryhodný digitální dokument – Stanovisko ICT UNIE k problematice právně validního dokumentu“ [2].

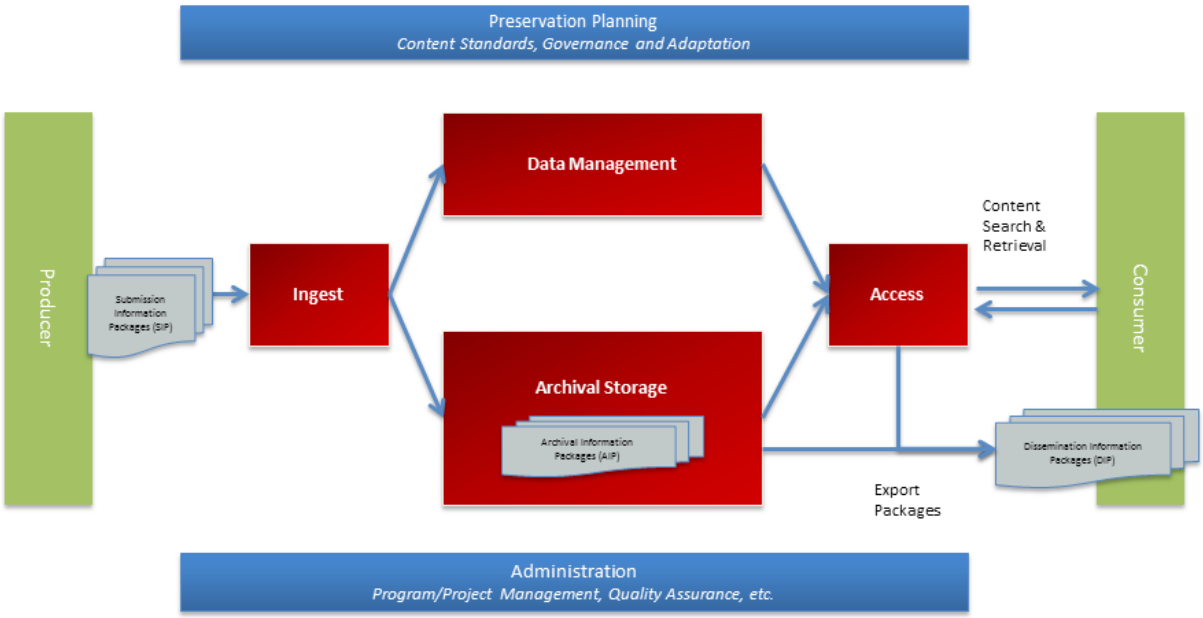
4 SLUŽBY PRO SPRÁVU A UCHOVÁVÁNÍ DŮVĚRYHODNÝCH DOKUMENTŮ

Pro správu a uchovávání důvěryhodných dokumentů je třeba řešit minimálně následující problematiky:

- službu fixace dokumentu formou elektronické značky/podpisu a/nebo časového razítka;
- službu převodu dokumentu do standardizovaného archivního formátu;
- službu autorizované konverze, která by umožnila konvertovat i další formáty kromě PDF/A – minimálně AdES formáty;
- ověřování elektronické značky/podpisu;
- ověřování certifikátů, na nichž jsou založeny elektronický podpis/značka, časové razítko;
- řešení elektronické identity osob a jejich mandátu k podpisu dokumentů (mandátní registr);
- zachovávání/udržování síly kryptografického mechanismu elektronického podpisu/značky a časového razítka;
- potřebné služby a technologie elektronického úložiště z pohledu dlouhodobého ukládání informací – řízení přístupů (uživatelů/systémů), vytváření a ošetření logů systému – zabezpečení tzv. auditní stopy, řešení automatizovaných činností počínaje označováním dokumentů elektronickými značkami, časovými razítky, jejich validací apod.;
- volbu vhodných zálohovacích mechanismů.

5 ŘEŠENÍ DŮVĚRYHODNÉ ELEKTRONICKÉ ARCHIVACE

Ideální řešení vychází z referenčního modelu OAIS a je založeno na rozdělení systému elektronické archivace na dvě základní části řešení: logická (softwarová) část starající se o procesy v archivu a fyzická (hardwarová) část starající se o bezpečné uložení dat. Mezi základní charakteristiky takovéhoto řešení patří otevřenost, transparentnost a strukturovanost.



Obrázek – Referenční model OAIS

5.1 Logická vrstva elektronické archivace

Logická (aplikační/softwarová) vrstva elektronické archivace je tvořena komponentou důvěryhodného elektronického archivu, který se stará o zachování důvěryhodnosti uložených elektronických dokumentů, resp. jejich elektronických podpisů, značek (pečetí) a časových razítek. Elektronicky uložený dokument se dá, dle evropské i české legislativy, **pokládat za důvěryhodný**, je-li opatřen **platným elektronickým podpisem a kvalifikovaným časovým razítkem. Při zachování platnosti těchto prvků elektronického zabezpečení a neporušenosti datové integrity, tj., že kontrolní součty vypočtené z obsahu odpovídají kontrolním součtům vypočteným v době podpisu, se dá takovýto dokument pokládat za důvěryhodný bez ohledu na formu jeho fyzického uložení.**

5.1.1 Digitální kontinuita a důvěryhodnost dokumentu

Dlouhodobé uložení dokumentů podepsaných elektronickým podpisem založeným na kvalifikovaném certifikátu implikuje potřebu řešit problém omezené platnosti tohoto certifikátu. S nezanedbatelnou pravděpodobností se může stát, že v době, kdy je potřeba prokázat důvěryhodnost dokumentu, může být certifikát, na kterém je podpis založen, již neplatný (ať už z důvodu vypršené stanovené platnosti, nebo účelné revokace z důvodu kompromitace samotného certifikátu). Při současném využití elektronického časového razítka je však možné platnost certifikátu podpisu prokazovat k času orazítkování, kdy byl certifikát ještě platný.

Kvalifikovaný certifikát, na kterém je založeno časové razítko, má však také omezenou platnost. Toto omezení lze spolehlivě řešit procesem přerazítkování, kdy je dokument opatřen novým časovým razítkem vždy před vypršením platnosti certifikátu posledního časového razítka.

Ani tím však není zcela zaručena prokazatelnost důvěryhodnosti dokumentu. Informace použité pro ověření dokumentu v čase označení časovým razítkem mají také omezenou platnost. Jedná se především o CRL seznamy certifikačních autorit, odpovědi OCSP služeb, použité certifikáty a jejich hierarchickou strukturu. Řešením je uložení všech informací použitých pro ověření spolu s ověřovaným dokumentem do struktury k tomu určené – archivního balíčku. Vhodné datové struktury definují ETSI standardy rozšířeného elektronického podpisu AdES. Tyto datové struktury zároveň odpovídají požadavkům na AIP balíček standardu OAIS.

Těmito **referenčními** (rozhodnutí Evropské komise 2011/130/EU) formáty jsou **CAdES, PAdES** a **XAdES**. Jedná se o formáty, které vznikly v rámci Evropského institutu pro telekomunikační standardy (ETSI – European Telecommunications Standard Institute). Tyto normy ETSI detailně definují, jak má být připojen elektronický podpis a časové razítko (výpočty kontrolních součtů /hashů/, šifrování, opatřování metadaty apod.).

- ETSI TS 103172 v2.2.2 – PAdES
- ETSI TS 103173 v2.2.1 – CAdES
- ETSI TS 103171 v2.1.1 – XAdES
- ETSI TS 103174 v2.2.1 – ASiC

Z norem ETSI také jednoznačně vyplývá, jak má proces dlouhodobé archivace dokumentu probíhat:

1. Kontrola platnosti elektronických podpisů připojených k dokumentu. To zahrnuje neporušenost kontrolního součtu a platnost certifikátu.
2. Připojení metadat: aktuální verze CRL (seznam zneplatněných certifikátů), OCSP odpovědi, případně další.
3. Připojení časového razítka tak, aby kontrolní součet chránil nejen samotný dokument, ale i jeho metadata.
4. Periodické připojování dalších časových razítek tak, aby každé další bylo připojeno před vypršením platnosti předchozího.

Způsob provedení každého z těchto úkonů je detailně specifikován ve zmíněných normách ETSI.

5.1.2 Validace dokumentu

Dokument podepsaný osobním elektronickým podpisem založeným na kvalifikovaném certifikátu nebo označený elektronickou systémovou značkou založenou na kvalifikovaném certifikátu je tímto bezpečnostním prvkem zafixován. V rámci systému elektronické archivace se musí kontrolovat platnost certifikátu, na kterém je podpis založen. Validace certifikátu spočívá v kontrole, zda jej vydala důvěryhodná autorita, zda je certifikát platný a nebyl uveden na seznamu zneplatněných certifikátů certifikační autority. V rámci kontroly je provedeno porovnání s CRL seznamy certifikačních autorit a vyhodnocení, zda použité certifikáty byly k testovanému datu platné. Vzhledem k časové prodlevě mezi odvoláním certifikátu a vydáním a zpracováním CRL je nutné pro rozhodnutí o platnosti certifikátu vyčkat tak dlouho, aby byly vráceny údaje o platnosti založené na CRL listu, jehož *platnost od* je až po čase, ke kterému se o platnosti certifikátu rozhoduje. Systém musí podporovat nejméně validaci certifikátů akreditovaných certifikačních autorit vedených v Trusted Service List (TSL) příslušných států Evropské unie.

5.1.3 Sdružování archivovaných dokumentů

Z pohledu produkční dlouhodobé archivace elektronických dokumentů je nutná podpora tvorby archivních balíčků zajišťujících dlouhodobou platnost celé sady dokumentů, což vede k optimalizaci procesu razítkování a přerazítkování dokumentů tak, aby byly minimalizovány náklady na razítka od časové autority. Systém balíčkování musí splňovat minimálně následující vlastnosti:

- možnost balíčkování dokumentů do jednoho archivního balíčku nezávisle na jejich typu, významu, různých přístupových právech a bez jejich vzájemného vztahu;
- poskytování důkazních informací k jednotlivým dokumentům bez nutnosti znalosti obsahu ostatních dokumentů ve stejném archivním balíčku;
- možnost mazat z archivu dokumenty, aniž by byla ovlivněna schopnost prokázání platnosti ostatních dokumentů ošetřených stejným archivním balíčkem.

Základní idea řešení vychází z možností zmiňované struktury XAdES:

- specifikace množiny podepisovaných objektů;
- výběr nejsilnějšího podporovaného hash algoritmu, aktuálně se jedná o SHA-512;
- pro každý podepisovaný objekt výpočet hash hodnoty definovaným způsobem (kanonizace, transformace, výpočet);
- vytvoření XAdES s použitím ds:Manifest elementů pro vložení vypočtených hash hodnot. Všechny podepisované objekty jsou zařazeny do jednoho ds:Manifest elementu, který je referencovaný jedním ds:Reference elementem;
- používat detached signature (podepisované objekty /dokumenty/ jsou mimo XML s XAdES podpisem);
- mechanismus vnořování existujícího balíčku do nově vytvářeného balíčku.

5.1.4 Podpůrné funkce a procesy

Skartace dokumentů

Skartace dokumentů je důležitou částí životního cyklu **papírových dokumentů**. Důvodem byl a je neudržitelný objem archivovaných dokumentů a z něho vyplývající potřeba zbavit se těch nadbytečných a nepotřebných. V elektronickém světě však tento důvod neplatí. S kapacitou datových úložišť rostoucí geometrickou řadou se naopak prostor potřebný pro uchování elektronických dokumentů snižuje. Ve své podstatě tedy skartace elektronických dokumentů není potřebná. Jako ideální se naopak jeví uchovávat všechny archivované dokumenty po neomezeně dlouhou dobu.

Protože však ještě nějakou dobu bohužel přetrvají zvyky, způsoby a procesy ze světa papíru, je třeba alespoň po přechodnou dobu tento proces umožnit i ve světě elektronickém. Logická vrstva archivu by proto měla podporovat nebo přímo řídit proces skartace.

Evidence

Logická vrstva archivu si vede nezávisle index obsahu uloženého ve fyzické vrstvě.

5.2 Fyzická vrstva elektronické archivace

Ukládání důvěryhodných dokumentů do datového úložiště se z pohledu fyzické vrstvy nijak neliší od ukládání jakéhokoliv jiného dokumentu. Důvěryhodný dokument tedy může být uložen kdekoliv, protože jeho důvěryhodnost je vyřešena na úrovni dokumentu samotného. Z praktického hlediska tak může v jednom okamžiku existovat nekonečné množství identických dokumentů uložených na nejrůznějších místech, datových úložištích datových center, úložištích elektronických poštovních systémů, zálohovacích zařízeních datových center nebo pouze v lokálním úložišti osobního počítače, notebooku, tabletu nebo mobilního telefonu.

Ze všech zmíněných typů úložišť však lze dokument jednoduchým, případně mírně komplikovanějším postupem smazat – odstranit tak, že právě ta konkrétní jeho „kopie“ přestane existovat. Pokud by došlo ke smazání všech kopií důvěryhodného dokumentu, pokud by došlo k situaci, že přestanou existovat veškeré jeho identické kopie umístěné v celosvětovém kybernetickém prostoru, pak může nastat řada situací s dalekosáhlými právními následky a bylo by dobré mít vždycky minimálně jednu kopii důvěryhodného dokumentu uloženou na místě, kde její smazání není snadné nebo je dokonce nemožné.

Také v okamžiku, kdy je důvěryhodný dokument prohlášen za archiválii, je nutné ho uložit do speciálního typu úložiště, se speciálními vlastnostmi, kde bude zaručeně existovat po definovanou nebo dokonce nekonečnou dobu tak, aby byl kdykoliv v budoucnosti přístupný. Speciální úložiště pro takové typy dokumentů lze zjednodušeně nazvat „dlouhodobým úložištěm“. V historicky ne příliš vzdálené minulosti se můžeme setkat s pojmem „garantované úložiště“, který byl používán v projektu technologických center krajů, IOP 08

(viz http://extranet.kr-vysocina.cz/download/odbor_informatiky/projekty/iop/ZD_TCK_ver9.pdf).

V dalším textu budeme pracovat pouze s pojmem „dlouhodobé úložiště“ nebo také DÚ.

5.2.1 Základní vlastnosti dlouhodobého úložiště

Setkáváme se často s otázkami: Jaké by měly být základní vlastnosti takového úložiště? Které vlastnosti jsou pro správné nakládání s dokumenty zásadní a které naopak přináší pouze např. vyšší komfort? A existují dnes na trhu speciální typy úložišť, které by se daly jako DÚ používat?

Zásadní požadavky na DÚ:

1. **Vysoká bezpečnost, neměnnost informací** – Garantovaná autentičnost a nepodvržitelnost obsahu archivu (certifikace US SEC 17 CFR 240.17a-4, certifikáty EU). Uložené dokumenty jsou od okamžiku zápisu do DÚ garantovaně neměnné. Data v úložišti musí být chráněna proti ztrátě nejméně metodou existence více nezávislých kopií v zařízení. V lepším případě jsou pak aplikovány další mechanismy zabraňující ztrátě nebo změně dat způsobené technickou chybou, jako jsou např. paritní a cyklické kódy. Dále musí zařízení podporovat definovatelné intervaly, po které je garantováno, že uložený dokument nemůže být uživatelským zásahem smazán a ani nijak pozměněn (retenční doba). Doba retence musí být nastavitelná také na základě definované události. Mazání dokumentů z úložiště musí být auditovaný proces, který podléhá definovaným pravidlům skartace. Dále musí úložiště garantovat, že nelze vnějším zásahem manipulovat se systémovým časem a ovlivnit tak nastavené retenční doby.
2. **Mazání dokumentů** – Smazat dokument lze pouze auditovatelným způsobem – v rámci DÚ existuje pouze garantovaný skartační algoritmus.
3. **Rozšiřitelnost** – DÚ umožňuje bezproblémovou a dlouhodobou rozšiřitelnost realizovatelnou bez ohrožení uložených dat. DÚ má modulární konstrukci, každý modul disponuje určitou úložnou kapacitou. Interní systém je vystavěn na standardech, aby jej po uplynutí životnosti jednotlivých modulů bylo možné osadit novými moduly. Zároveň musí být jasně definován proces migrace dat v případě upgradu na novější verze.
4. **Replikace dat** – DÚ je vybaveno systémem pro replikaci dat. Přestože je dlouhodobé úložiště vybaveno systémem vysoké dostupnosti, který znamená, že dokumenty na něm uložené existují současně minimálně ve dvou identických kopiích, je nutné, aby DÚ dokázalo provádět replikaci dat do jiného identického zařízení geograficky v jiné lokalitě. Sekundární, případně n-tá lokalita musí být schopna dočasně převzít veškeré funkce lokality primární, jak z pohledu přístupu k uloženým dokumentům, tak z pohledu ukládání nových dokumentů.
5. **Pokročilá organizace dat** – Data v úložišti musí být možné organizovat do virtuálních prostorů s odděleným nastavením.

Všechny další vlastnosti zlepšují funkcionality DÚ, ale pro jeho funkci nejsou bezpodmínečně nutné. Patří k nim např.:

1. komprese a deduplikace;
2. spin-down;
3. nepřetržitý monitoring stavu.

5.2.2 Trh IT z pohledu DÚ v současnosti

V minulosti existovalo pouze jediné řešení, které by mohlo aspirovat na post fyzického úložiště pro DÚ. Jeho vlastnosti jsou jednoznačně popsané použitou technologií WORM (Write Once Read More), tedy jednou zapsaná data pak slouží už pouze ke čtení bez fyzické (technologické) možnosti je jakkoliv modifikovat. Technologie je dosud využívána u magnetopáskových jednotek a pro DÚ je podle našeho názoru nepoužitelná, stejně jako nejrůznější magnetooptické jednotky. U těch je navíc dostupnost v České republice minimální, možná spíše nemožná. Magnetopáskové a magnetooptické jednotky už jenom díky komplikované manipulaci se záznamovými médii, jejich nízké spolehlivosti a nutnosti pracovat vždy s větším množstvím fyzických médií, která obsahují totožná data (aby se zamezilo ztrátě dat při poruše média), mají omezené možnosti pro nasazení jako DÚ. Jejich spojení se SW vrstvou i díky předchozí komplikaci může být velmi náročné.

V současné době lze najít dva základní směry, kterými se výrobci řešení pro DÚ ubírají. Prvním je čistě HW platforma, která nabízí množství přístupových protokolů pro své využití a všechny zásadní funkce jsou integrované v operačním systému tohoto zařízení. Druhým je pak soubor HW a SW komponent, ze kterých se DÚ dá vybudovat.

Čistě HW řešení:

Speciální architektura (Content Addressed Storage), která se liší od standardních diskových úložišť – elektronické dokumenty jsou ukládány na základě svého obsahu (content), a tím je zabezpečena jedinečnost a autenticita uložených dokumentů. Jednoduše řečeno – s dokumentem se ukládají i další informace jako jakási obálka, která uchovává množství informací v dokumentu neuložitelných. Zabezpečuje tak dlouhodobé uchování, vynucení archivačních a skartačních politik, zabezpečuje autorizovaný přístup, audit, a to vše na HW úrovni. Vlastník procesu archivace tak dostává do ruky nástroj, díky kterému se může soustředit pouze na definici a správu politik a garanci neměnnosti obsahu za něj řeší zařízení samo.

HW zařízení umožňuje správcům transparentní definici politik, jednoduchou správu, která je oddělena od správy obsahu. Používaná rozhraní jsou dle standardu SNIA XAM (XAM v1.0.1 ANSI standard, http://www.snia.org/forums/xam/technology/standards/), který je speciálně navržen pro dlouhodobou archivaci neměnného obsahu a může se tedy velmi jednoduše integrovat s aplikacemi přímo určenými pro archivaci. Dále obsahuje standardní JAVA nebo C# API, na které je možno se napojit. Dále je možno zařízení zapojit do infrastruktury jako souborový server, jehož jednotlivé adresáře respektují definované politiky a data, která jsou tam aplikacemi ukládána, pak těmto politikám podléhají.

Díky speciálnímu mechanismu ukládání dat je uložený obsah ochráněn proti zneužití.

Z výše uvedeného plyne, že zařízení je speciálně určeno pro dlouhodobé uložení dokumentů (nebo obecně obsahu) za účelem garance bezpečného fyzického uložení. Typické použití je pro systémy spisových služeb (nebo obecně Records Management systémů), speciálních archivních a zálohovacích systémů, systémů pro správu a oběh dokumentů, systémů pro řízení životního cyklu dokumentů, ekonomických informačních systémů, nemocničních informačních systémů a mnoha dalších.

Speciální verze HW produktů jsou navrženy pro uchování dat, která podléhají speciálním zákonům (ne v České republice) upravujícím nakládání s daty (např. SEC Rule 17a-4, 21CFR Part 11, HIPAA, Sarbanes-Oxley, GoBs, DoD 5015.2, Moreq II, ISO/IEC 25051).

Kombinace HW a SW řešení:

Existuje několik řešení dlouhodobého úložiště, opírajících se o kombinaci HW a SW komponent, která dohromady plní požadované funkce. Liší se od sebe použitými technologiemi, ale obecně se dá říci, že se vždy jedná o servery s interní diskovou kapacitou (např. platforma x86) a na nich buďto přímo jako operační systém, nebo jako aplikace v operačním systému běží SW komponenty dávající zařízení stejné nebo alespoň podobné vlastnosti, jaké nalézáme u čistě HW řešení.

V současné době se jeví jako vhodnější řešení typu „**appliance**“ (**dokonale sladěné zařízení od jednoho dodavatele**), a to především díky integrovaným systémům, které dokážou dlouhodobě zaručit případnou migraci dat uvnitř systému z technologicky starší na novější HW platformu, aniž by utrpěla kterákoliv jiná vlastnost takového DÚ.

6 SHRNUTÍ

Elektronicky uložený dokument se dá, dle evropské i české legislativy, pokládat za důvěryhodný, je-li opatřen platným elektronickým podpisem, značkou/pečetí organizace a kvalifikovaným časovým razítkem. Při zachování platnosti těchto prvků elektronického zabezpečení a neporušenosti datové integrity, tj., že kontrolní součty vypočtené z obsahu odpovídají kontrolním součtům vypočteným v době podpisu, se dá takovýto dokument pokládat za důvěryhodný bez ohledu na formu jeho fyzického uložení.

Bez bezpečného fyzického uložení ovšem hrozí riziko poškození, neoprávněné změny či smazání důvěryhodných dokumentů a tím jejich ztráta.

Optimálním řešením při budování dlouhodobých důvěryhodných archivů či úložišť je spojení logické vrstvy, zajišťující a prokazující důvěryhodnost původu a obsahu dokumentu a vrstvy fyzické zajišťující jejich dlouhodobé bezpečné fyzické uložení.

Velkým problémem České republiky v současné době je, že neexistuje dostatečně propracovaný certifikační postup ani neexistuje autorita, která by byla schopná a kompetentní posoudit produkty jednotlivých výrobců a prohlásit je za vyhovující pro dlouhodobou důvěryhodnou archivaci. Můžeme se spolehnout na mezinárodní standardy a certifikáty např. EU nebo USA anebo je třeba definovat a nastavit vlastní, společně se zřízením odpovídající české autority, která bude opravdu schopná některá řešení jako důvěryhodná úložiště certifikovat.

Z druhé strany existují i důležité projekty, které se věnují auditu digitálních repozitářů, který by byl nezbytný pro jejich certifikaci. Jsou to například NESTOR, TRAC, DRAMBORA a PLATTER.

NESTOR (Nestor Catalogue of Criteria for Trusted Digital Repositories) – nástroj pro interní audit, poskytující návod pro budovatele digitálních repozitářů a vytvářející současně tlak na dodržování aktuálních standardů. [6]

TRAC (Trustworthy Repositories Audit & Certification) – nástroj v podobě „checklistu“ (seznamu), s doporučujícími postupy nezbytnými pro budování důvěryhodného repozitáře. Vychází z modelu OAIS. [7]

DRAMBORA (Digital Repository Audit Method Based on Risk Assessment) – využívá principu sebehodnocení a interního auditu, vyhledává slabá místa a upozorňuje na rizika. [8]

PLATTER (Planning Tool for Trusted Electronic Repositories) – „kuchařka“ pro projekty digitálních repozitářů poukazující na rozsah problematiky a upozorňující na rizika a potenciální problémy. [9]

7 NAVAZUJÍCÍ AKTIVITY PRACOVNÍ SKUPINY ICTU – ARCHIVNICTVÍ

7.1 Pracovní tým Důkazní materiál

Činnost pracovního týmu „Důkazní materiál“ navazuje na pracovní tým „Správa a ukládání důvěryhodných dokumentů“. Jelikož je potřebné u digitálních dokumentů prokazovat také jejich důvěryhodnost, a to jak v civilním, tak i ve správním či trestněprávním prostředí, rozhodli se členové týmu Důkazní materiál navrhnout standardní způsob prokazování této důvěryhodnosti. Činnost týmu je rozdělena do dvou samostatných částí – navržení technické stránky řešení a návrh na změny v legislativě tak, aby právě navržené řešení zjednodušilo způsob prokazování důvěryhodnosti daného dokumentu.

8 POUŽITÁ LITERATURA

1. **Rosenthal, C., A. Blekinge-Rasmussen, J. Hutař a kol.**
   Průvodce plánem důvěryhodného digitálního repozitáře (PLATTER).
   Praha: Národní knihovna České republiky, 2009.
2. **DRAMBORA interactive.**
   ***Digital Repository Audit Method Based on Risk Assessmen* [online].**
   Dostupné z: http://www.repositoryaudit.eu/.
3. **Hloušková V., J. Lubas, I. Rosol a B. Bobčík**.
   Důvěryhodný digitální dokument. Stanovisko ICT UNIE k problematice právně validního dokumentu.
   Praha: ICT UNIE, 2014.
4. **Central European Advisory Group.**
   ***ELEKTRONICKÁ ARCHIVACE* [online]. 2007.**
   Dostupné z: http://www.digiarchiv.cz/?type=uvod.
5. **United Nations Commission on Internationa Trade Law. UNCITRAL Model Law on Electronic Commerce (1996) with additional acrticle 5 bis as adopted in 1998.**
   ***UNCITRAL* [online].**
   Dostupné z: http://www.uncitral.org/uncitral/uncitral_texts/electronic_commerce/1996Model.html.
6. **Machotka, Jiří. Garantované vs. Negarantované úložiště (Dlouhodobé ukládání dokumentů).**
   ***Oracle Czech WebCenter Blog* [online]. 19. listopadu 2009.**
   Dostupné z: http://oraclecze20.blogspot.cz/2009/11/garantovane-vs-negarantovane-uloziste.html.
7. **eIDAS ammendments consolidated text voted in European Parliament.**
   ***CERTIFIED ELECTRONIC SIGNATURE* [online]. 14. duben 2014.**
   Dostupné z: http://certifiedsignature.eu/2014/04/14/texto-consolidado-de-enmiendas-de-eidas-votado-en-el-parlamento-europeo/.
8. **Geschäftsstelle Deutsche Nationalbibliothek.**
   Nestor [online].
   Dostupné z: http://www.langzeitarchivierung.de/Subsites/nestor/EN/Header/Kontakt/kontakt_node.html.
9. **CRL, The Center for Research Libraries and OCLC Online Computer Library Center, Inc.**
   Trustworthy Repositories, Audit and Certification: Criteria and Checklist [online]. 2007.
   Dostupné z: http://www.crl.edu/sites/default/files/d6/attachments/pages/trac_0.pdf.

Na zpracování dokumentu se podíleli členové pracovní skupiny Archivnictví:

Jaroslav Lubas, Petr Kubíček, Jan Tejchman.

Poznámka autorského kolektivu

Při tvorbě tohoto dokumentu autoři vycházeli ze současné právní úpravy a technických standardů ČR a EU, ze zkušeností a praxe různých členských států EU a také z historických zvyklostí a právních premis.

Autoři si jsou vědomi, že „důvěryhodnost“ konkrétního dokumentu jakožto důkazního prostředku v soudním řízení může určit pouze soud.

Materiál je k dispozici v elektronické podobě na webových stránkách ICT UNIE – **www.ictu.cz**.

ICT UNIE z.s.
K Červenému dvoru 25a/3269
130 00 Praha 3
tel.: +420 222 582 880
info: ictu@ictu.cz
www.ictu.cz